

# PathQuoteSpaces

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Cigital, Inc.

2007-04-02

## Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4133 bytes

Attack Category	<ul style="list-style-type: none"><li>• Malicious Input</li></ul>		
Vulnerability Category	<ul style="list-style-type: none"><li>• Buffer Overflow</li><li>• Unconditional</li></ul>		
Software Context	<ul style="list-style-type: none"><li>• String Management</li><li>• String Parsing</li></ul>		
Location	<ul style="list-style-type: none"><li>• shlwapi.h</li></ul>		
Description	<p>The destination string buffer for the PathQuoteSpaces() function must be long enough to hold the return file path.</p> <p>The PathQuoteSpaces() routine searches the string for spaces. If they are present, it adds quotation marks at the beginning and end of the string. If spaces are present, it will expand the string by at most two characters. The string buffer must be large enough to accommodate these extra characters.</p>		
APIs	Function Name		Comments
	PathQuoteSpaces		
	PathQuoteSpacesA		ANSII implementation
	PathQuoteSpacesW		Unicode implementation
Method of Attack	<p>This routine could potentially expand the input string by two characters (quotation marks on beginning and end). If the string is not declared to have extra space, it could overflow the buffer. This could allow an attacker to crash the program or potentially exploit a buffer overflow problem. However, since the routine will overflow at most two characters, there is limited ability to do anything particularly dangerous.</p>		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Whenever PathQuoteSpaces() is used.	The buffer is referred to by the sole	Effective.

1. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/35-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html) (Barnum, Sean)

		parameter must have room for at least two additional characters. Best practice is to ensure that the buffer is at least MAX_PATH +2 characters in length.	
<b>Signature Details</b>	void PathQuoteSpaces(LPTSTR lpsz);		
<b>Examples of Incorrect Code</b>	<pre>TCHAR path[] = TEXT("C:\\Program Files\\Foo"); // Note: Buffer is too small and will overflow LPTSTR lpsz = path; PathQuoteSpaces(lpsz);</pre>		
<b>Examples of Corrected Code</b>	<pre>TCHAR path[MAX_PATH+2] = TEXT("C:\\Program Files\\Foo"); // Note: Buffer is correctly sized LPTSTR lpsz = path; PathQuoteSpaces(lpsz);</pre>		
<b>Source Reference</b>	<ul style="list-style-type: none"> <li><a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/shlwapi/path/pathquotespaces.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/shlwapi/path/pathquotespaces.asp</a><sup>2</sup></li> </ul>		
<b>Recommended Resource</b>			
<b>Discriminant Set</b>	<b>Operating System</b>	<ul style="list-style-type: none"> <li>Windows</li> </ul>	
	<b>Languages</b>	<ul style="list-style-type: none"> <li>C</li> <li>C++</li> </ul>	

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at [copyright@cigital.com](mailto:copyright@cigital.com)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>